DHS Official Seeks to Reassure Senate Panel That Cybersecurity Performance Will Improve

7/20/05- E & E Daily (www.eedaily.com)

The Homeland Security Department takes its leadership role in ensuring national critical infrastructure cybersecurity very seriously and is taking steps to increase its commitment of resources to that effort, Andy Purdy, acting director of the DHS National Cyber Security Division, told a Senate panel July 19.

Purdy's testimony sought to reassure members of the Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Federal Financial Management, Government Information, and International Security, who expressed concerns about the effectiveness of DHS cybersecurity efforts.

At the same hearing, Thomas M. Jarrett, secretary of Delaware's Department of Technology and Information and president of the National Association of State Chief Information Officers, told the panel that "cyberspace is the only part of the nation's critical infrastructure that is under attack everywhere, all of the time."

The number of attacks on state information systems and resulting costs to states is rising dramatically, Jarrett said, adding that approximately 15 percent of his state department budget is dedicated to cybersecurity. Jarrett noted that a recent study by North Carolina demonstrated that some $50 million dollars per year would be necessary to implement an effective cybersecurity program in the state.

Jarrett said that information sharing between the states and DHS has to date been difficult. He urged the subcommittee to take action to ensure a closer joint cybersecurity effort by the federal government and the states. Jarrett also expressed concern that the level of federal funding for cybersecurity may be insufficient.

Senators Express Concern

Subcommittee Ranking Minority Member Sen. Thomas R. Carper (D-Del.) said that the recent London transportation system bombings demonstrated that "terrorists will seek to exploit vulnerabilities" and said that critical infrastructure cybersecurity is perceived by many as a current vulnerability.

The recent wave of data breach incidents in which millions of U.S. citizens faced the unauthorized release of their personal information shows just how attractive a target information databases have become, commented Sen. Daniel K. Akaka (D-Hawaii).

Subcommittee Chairman Tom Coburn (R-Okla.) said that banking and financial services sector leaders had made clear that as yet they do not feel they can rely enough on DHS as a partner in cybersecurity efforts.

Purdy said that with the creation of a new DHS cybersecurity assistant secretary position "we are confident that we will accelerate our cybersecurity efforts."

Purdy's reference was to the July 13 announcement by Homeland Security Secretary Michael Chertoff that DHS will undergo a series of organizational changes including adding an assistant secretary for cybersecurity.

David Powner, director of IT management for the General Accountability Office, said that while the plan to add a cybersecurity assistant secretary position is a positive step, the real challenge will be for DHS to adequately staff and provide adequate resources for the National Cyber Security Division that the assistant secretary will lead.

GAO Cybersecurity Findings Discussed

Sens. Coburn and Carper both cited a recent GAO report that found DHS had not yet met any of its primary cybersecurity responsibilities.

GAO concluded in the report, which was made public June 27, that DHS faces numerous challenges, including establishing organizational stability and authority, overcoming hiring and contracting issues, and demonstrating the value it can provide in leading the cybersecurity effort.

GAO's Powner reasserted the report's conclusions in his testimony to the subcommittee. Power emphasized that some industry sectors told GAO that there is an insufficient level of trust between the private sector and DHS on information sharing efforts to strengthen cybersecurity.

Powner reemphasized GAO's recommendation that DHS work to prioritize its list of cybersecurity duties.

Asked by Coburn whether DHS was engaged in such a prioritization effort, Purdy said that prioritization issues are part of the department's overall cybersecurity effort and are part of creating a National Infrastructure Protection Plan (NIPP).

He said that "a pretty good" draft NIPP should be available by the end of the summer but admitted that a more complete report that included implementation milestones and performance measures may not be ready before the end of the year.

Purdy said that the department reorganization announced by Chertoff would not delay the release of the NIPP.

Meanwhile, the GAO released a report July 15 that concluded cybersecurity efforts at 24 major federal agencies remain incomplete and are characterized by "pervasive weaknesses" that put federal information and operations "at risk of fraud, misuse, and destruction."

The National Institute of Standards and Technology July 15 released a new draft Federal Information Processing Standard setting "Minimum Security Requirements for Federal Information and Information Systems."

Further information on the hearing,"Securing Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges," including the written testimony of witnesses, is available at
http://hsgac.senate.gov/index.cfm?Fuseaction=Hearings.Detail